Interdisciplinary Description of Complex Systems 18(3), 327-336, 2020

RISK-ADAPTED ACCESS CONTROL WITH MULTIMODAL BIOMETRIC IDENTIFICATION

Gábor Werner[1], * and László Hanka[2]

[1]Óbuda University, Applied Biometric Institute
Budapest, Hungary

[2]Óbuda University, Institute of Mechatronics and Autotechnics
Budapest, Hungary

DOI: 10.7906/indecs.18.3.1
Regular article

Received: 31 January 2019.
Accepted: 3 March 2020.

ABSTRACT

The presented article examines the background of biometric identification. As a technical method of authentication, biometrics suffers from some limitations. These limitations are due to human nature, because skin, appearance and behavior changes more or less continuously in time. Changing patterns affect quality and always pose a significantly higher risk. This study investigated risk adaption and the integration of the mathematical representation of this risk into the whole authentication process. Several biometrical identification methods have been compared in order to find an algorithm of a multimodal biometric identification process as a possible solution to simultaneously improve the rates of failed acceptations and rejections. This unique solution is based on the Adaptive Neuro-Fuzzy Inference System and the Bayesian Theorem.

KEY WORDS

multimodal biometrics, artificial intelligence, ANFIS, risk management

CLASSIFICATION

ACM: Security and privacy, Biometrics
JEL: Z13

*Corresponding author, η: wga.bme@gmail.com; +36 20 411 8184;
Hungary 1034 Budapest, Bécsi út 96/b

INTRODUCTION

The modern world is surrounded by hidden layers of authentication protocols. Independent from the professional, governmental or private sphere, there is information that has a different value for users. This value sometimes is not objective, therefore, some information may be worthless for some, while others could not live without it. As the amount of personal information and linkages among components are growing, the security behind data management becomes a crucial issue.

In highly secured systems there are strict protocols for access privileges. These protocols involve the use of difficult passwords, multifactor authentication, two key encryption, etc. Nevertheless, there are common attributes in these techniques; they are quite complicated, and it is necessary for all users to know a unique key (password) or to own a hardware (tag) to complete identification.

Biometrics has a history in identification in the field of forensics, rather than in encryption. For instance, the first mobile phone with fingerprint reader on the market was the Toshiba G500 in 2007, but the large-scale spread started with the iPhone 5s in 2012, and nowadays almost all middle class mobile phones are equipped with an inbuilt fingerprint reader, and according to the latest developments the newest generations of smartphones will not have any separate fingerprint readers, instead it is going to be built into the screen [1]. In the mobile market, in addition to the fingerprint reader biometrical technique, face recognition through the front camera, and voice recognition will be used as well. There are also some non direct biometrical traits that can be called personal identification samples, like movements of the user or the way of typing or browsing.

Whether the secured data is personal, official or governmental, the protection highly depends on the users and their skills. Usually a user has to remember several passwords and even correctly recall the correct positions of the letters, numbers or symbols. The user should not share it, lose it or save it onto a public surface. However, the human nature is less likely to be capable of remembering such a multitude of accurate sequences of codes, nor is it precise enough to handle a hardware tool, or it is simply inconvenient to do so.

The biggest challenges of the practical use of applied Biometrics are caused by the limitations above. Biometric identification seems to be more suitable, but it is still not used everywhere. The fact is, biometrics faces some social barriers, data encryption and storage challenges. However, the technical environment took a big step forward, – as it has been shown in the mobile market – as biometric contact is not only used for access control, it is becoming a live interaction between the machine and the user. For instance, in the not too distant future an autonomous car will be able to identify its drivers and even recognize the conditions and intentions of the drivers [2].

REVIEW OF RISK-ADAPTION

ROLE OF RISK

According to Haimes, risk management must be an integral part of decision making. As a system, biometric devices face hazards (malfunction, forced entry, terrorism, etc.) and all these have some consequences. The caused impact can be moral, confidential, financial or technological trauma. If risk management takes a part in the complete system engineering process, it will help to find the balance between the uncertain benefits and costs [3].

From a professional aspect, risk management is a tool which creates the opportunity to find the most suitable solutions and methods. For instance there are several access control techniques (RFID, keypad, biometrics, guard, etc.) that could be used when facing a given problem, but if the system-engineering does not take the real threats and significant consequences into consideration, the designed access control system might be inefficient or non-cost-effective.

MAIN ELEMENTS OF RISK CALCULATION

In a holistic risk assesment, basically all possible future states have to be taken into account, just like in an event tree analysis, which is a forward logical modeling technique for both success and failure states in the future. There are outcomes that are favorable and those that are not. From the initial state, regarding the circumstances, there is a likelihood of each future situation. Following Bayes' Theorem, each step has an aggregated likelihood from the priori elements, this is called conditional probability. Each element, step and impact has its exact place in the network of happenings. Risk calculation is a method where the significant effects and linkages are explored. In Haimes' terminology there are questions that have to be answered to set up the network [3]:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

The questions below investigate linkages between networks:

- What can be done and what options are available?
- What are the associated trade-offs in terms of all relevant costs, benefits and risks?
- What are the impacts of current management decisions on future options?

The last question is particularly important, because a poorly chosen management decision can restrain development, especially if the current factor is at the beginning of a sudden rising phase. For example, in the European Union since the Convention on Road Traffic (Vienna, 1968) autonomous cars not allowing human intervention have been banned, so manufacturers must still provide the possibility of human actions to drive.

MODELING RISK ANALYSIS

Risk management cannot be done without measurement and mathematical proceedings. The pareto optimum as an adequate goal of risk management is an intermediate point among the fitted descriptive functions. These function parameters and variables determine the optimum point. But in some cases it is difficult to determine these points, because of the attributions:

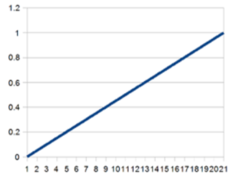	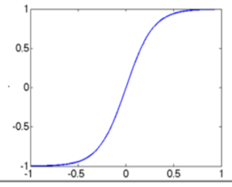	1. Linear vs. non-linear
$a, b, c, \ldots = \alpha, \beta, \gamma, \ldots$ $x, y, z, \ldots = \delta, \theta, \vartheta, \ldots$	$a, b, c, \ldots = P(\alpha), P(\beta), P(\gamma), \ldots$ $x, y, z, \ldots = P(\delta), P(\theta), P(\vartheta), \ldots$	2. Deterministic vs. stochastic
$a, b, c, \ldots = \alpha, \beta, \gamma, \ldots$ $x, y, z, \ldots = \delta, \theta, \vartheta, \ldots$	$a, b, c, \ldots = \alpha(t), \beta(t), \gamma(t), \ldots$ $x, y, z, \ldots = \delta(t), \theta(t), \vartheta(t), \ldots$	3. Static vs. dynamic
$a_i, b_i, c_i \quad i = 1, \ldots, n$	$a_i \quad i = 1$	4. Distributed parameters vs. lumped parameters

Figure 1. Attributions of risk analysis models.

Regarding the distinctive aspects above, different model types can be introduced as the following:

1) A linear model is one that is represented by linear equations. A nonlinear model is represented by nonlinear equations; that is, part or all of the constraints or the objective functions are nonlinear [3].

2) Deterministic models are those in which each variable and parameter can be assigned a definite fixed number or a series of fixed numbers for any given sets of conditions. In probabilistic (stochastic) models, neither the variables nor the parameters used to describe the input-output relationships and the structure of the elements (and the constraints) are precisely known [3].
3) Static models are those that do not explicitly take the variable time into account. Dynamic models are those involving difference or differential equations. Static optimization problems called mathematical programming, while dynamic optimization problems are often referred to as optimal control problems [3].
4) A lumped parameter model does not consider variations, and the various parameters and dependent variables can be considered to be homogeneous throughout the entire system. A distributed parameter model takes into account detailed variations in behavior from point to point throughout the whole system [3].

In Biometrics the background of risk assessment is more complex than the conventional index numbers anticipate. Common quality marks, like the rate of false acceptance (FAR) or false rejection (FRR) are only statistical results. To scientifically prove the compliance, it is necessary to get better involved, for example, by investigating the mathematical and physical model of the entire biometrical identification.

RISK-ADAPTION IN BIOMETRICS

As it is written by Jain et. al., in biometric identification there are several possibilities to cause an error in an authentication systems [4]. To understand the differences, errors must be distinguished. Two main kinds of error sources can be named: intrinsic failures and adversary attacks. An unintentional inner failure is caused by inadequate operation by the biometric device, so a user will be mistakenly rejected or accepted, even though he or she is not an impostor. The other set of errors are adversary attacks, which can aim at administration, the infrastructure or the users directly. In this study administrational and pattern theft from the user is less discussed compared to the direct attacks against the biometric system itself. A compromised system is facing two main threats: the secured objects will not be available to someone/anyone because the system breaks down, or an impostor gains entry into the system. From security aspects, these two sets of outcomes have important differences.

The Denial of Service Attack (DoS attack) as a classic hacking procedure is very similar to the first case. The basic idea in these cases is not about getting sensitive information or data, just merely preventing the operation of the service. For instance, if the operation is locking an access point, then there must be another entrance, or a safety key that could be used as a secondary option. So if there is a risk of DoS attack, the redundancy and the protection of the infrastructural parts becomes more crucial [5].

The other types of malicious actions are hacks. In our interpretation, hacking means a malicious act of an attacker intended to gather information or goods. According to Ratha, there are several points where an attacker can intervene into the biometrical authentication system. Four categories can be named; attacks on the user interface (input stage), attacks on the interface between modules, attacks on the modules, and attacks on the template database [6].

The vulnerability of the stages depend on many circumstances, such as time, preparedness of the attacker, the complexity of the algorithm, the dignity of the manufacturer and the responsible security personnel who applied or run the device. There are eight nominated points where an assault can be provided regarding the entire system of access control [6]:

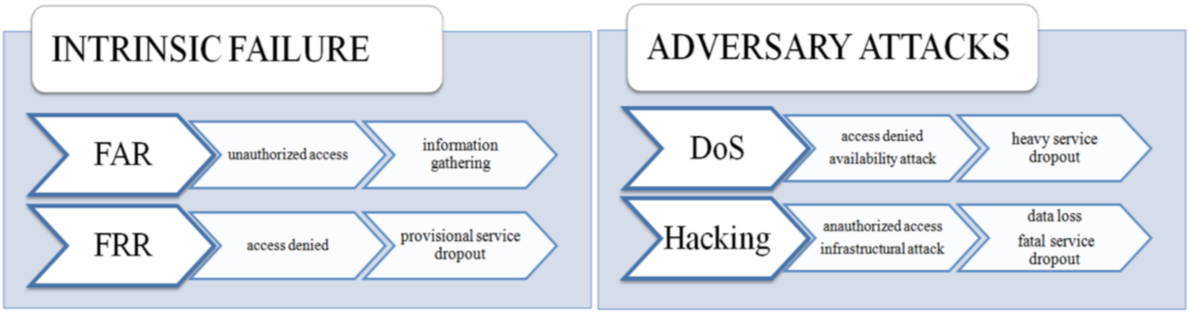
INTRINSIC FAILURE
FAR
unauthorized access
information gathering
FRR
access denied
provisional service dropout
ADVERSARY ATTACKS
DoS
access denied availability attack
heavy service dropout
Hacking
anauthorized access infrastructural attack
data loss fatal service dropout

Figure 2. Impact of the errors from different sources.

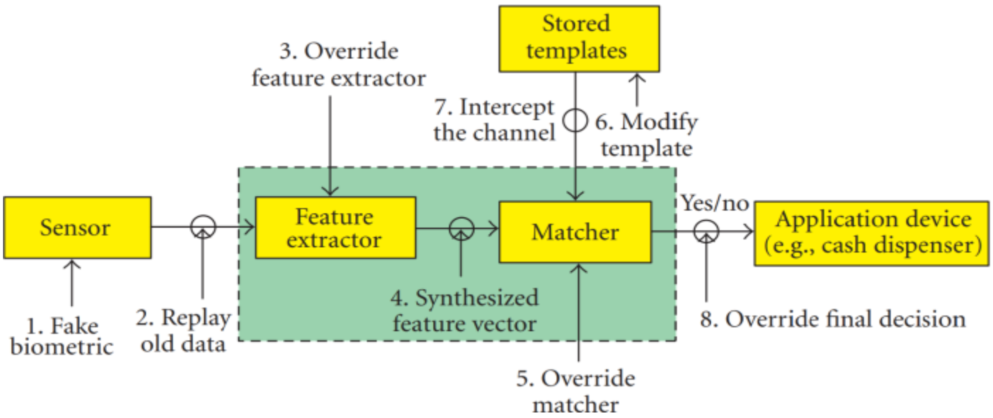

Figure 3. Possible points of attacks in a generic biometric system [6].

RISK MITIGATION POSSIBILITIES IN BIOMETRICS

As it was showed above, an impostor can intervene at several points in a biometric authentication system, including unsecured communication channels, algorithmic loopholes or even the physical design. From practical aspects, the protection of a secured access point (virtual of physical space) is characterized by the complexity of the security system, which should not be more expensive than the protected value, which can also mean reliabilty or personal trust.

In this case the total value approach must be applied, therefore, the complexity of the database management, the total spent time (denied access, error correction, etc.) and the costs of enhanced quality must be taken into consideration collectively. To determine the total cost, both the internal and the external effects have a significant impact, but it can be difficult to recognize and estimate some externalities, such as the social value.

In our case the chain model of the authentication process can be more precisely described by a mathematical model in which the vulnerability points are calculated as a multiplication instead of an addition. This assumption can be confirmed by the Bayes Theorem. Therefore, not only is the logical bond simpler, but also the roles of the attacked points are equal, which allows an easier comparison of different biometrical methods.

According to a study by Srivastava, biometric devices can be compared by many attributions, some of which have a significant role in value-based risk assessment [7].

Where the compared attributes are the following:

- Uniqueness: Each individual should have features but different from the other.
- Permanence: Biometrics should be sufficiently invariant over a certain period of time
- Universality: Population coverage; each individual should have a biometric feature.
- Measurability: Meaning simplicity of extraction and technical equipments..

- Comparability: Simplicity of comparison between templates and the sample.
- Collectability: How well can the identifiers be captured and quantified
- Invasiveness: Introduction of instrument into a body part.
- Performance: Accuracy, speed, security.
- Acceptability: To which extent is it supported by society.
- Circumvention: The act of cheating someone’s sample.

Table 1. Comparison of biometric methods [7].

	UNIQUENESS	PERMANENCE	UNIVERSALITY	MEASUREABILITY	COMPARABILITY	COLLECTABILITY	INVASIVENESS	PERFORMANCE	ACCEPTABILITY	CIRCUMVENTION
IRIS	H	H	H	M	M	H	M	H	M	L
RETINA	H	H	H	L	M	M	H	H	L	L
FINGERPRINT	H	H	M	H	M	M	M	M	H	M
PALMPRINT	H	H	M	H	M	M	M	M	H	M
HAND GEOMETRY	M	L	H	H	M	H	M	M	M	M
FACE	M	M	H	M	L	H	L	L	H	H
EAR	M	M	H	M	L	M	L	L	M	L
VOICE	L	L	M	M	L	M	L	L	H	H
KEYSTROKE	L	L	L	L	L	M	M	L	L	M
X-RAYED TEETH	L	L	M	L	L	M	H	L	L	H
SIGNATURE	H	L	L	M	M	H	M	M	H	H
DNA	H	H	H	L	L	L	H	H	H	L

Biometrical identification techniques differ, and they all have their pros and cons, and all techniques have a unique performance depending on the manufacturer. Furthermore, there are several types of algorithms for feature extraction and comparison, so the subset of applicable solutions is even more extensive.

As long as some identification methods theoretically can reach a very low FRR, in practice biometric techniques must face serious obstacles which derive from the extraction process of the biometric sample. This phenomenon can be named as ‘noisy interface’. The interface between the human and the machine will be contaminated with some noise in the normal signal. Some devices or the biometric identification methods themselves are sensitive to light, temperature, pollution, fine dirt, etc. These impacts have a high effect on the whole process, because the raw sample will be contaminated, so the distortion will be carried on throughout the whole authentication process. Thus in practical implementations, the environment must be taken into consideration whenever a new biometric device is introduced.

According to our assumption, with a series of data it is possible to statistically estimate the likelihood of the disturbing effects and find a suitable solution for identification.

Nevertheless, in many cases influential external impacts (noises) are not continuous or predictable. Thus if the specific error cannot be minimized, the result will be sensitive to extreme error values, and the FRR increases exponentially.

A good method to decrease the impact of a specific error is to divide it. The distributed specific error method can be implemented in such a situation with parallel multimodal biometric identification. To mitigate some risks, it is necessary to investigate the probability model of the authentication. Basically there are many components that have effects on the cumulated risk. In stochastic models, it is hardly possible to estimate by monitoring the components , the small changes in the user's behavior, environmental effects, etc., so it might be more appropriate to calculate with a multi-cumulated risk value. In order to have two or more cumulated risk values, the method of multimodality must be applied. These values are more discrete, so the summation is easier and there are working models for the calculations.

With regard to the research by John P. Baker at The Johns Hopkins University, it can be stated that the current biometric systems do not meet the performance requirements for high security applications, thus some fusion of multiple biometrics is being considered to help lower error rates. Some biometric systems use all available impressions sequentially until an acceptable match is obtained, while others include logical (AND/OR) operations as a summation of similarity scores. There are more sophisticated methods, that have been considered for combining scores from separate classifiers for each biometric modality using different feature extraction and matching algorithms to generate their scores [8].

METHODOLOGY OF THE MULTIMODAL SUMMATION

John P. Baker proposed a Bayesian belief network (BBN) based architecture for biometric fusion applications. The bayesian networks provide a unified probabilistic framework for optimal information fusion. The Bayesian methods have been used for a long time in biometrics, however the effectiveness and flexibility of the BBN has not been extracted. The networks based on the Bayesian theorem represent the joint probability distribution, where [9]:

$$P(X_1, \dots, X_n) = P(X_n) \prod_{i=1}^{n} P(X_i | parents(X_i)). \tag{1}$$

In the Baker study, the probability can be estimated by the quality, similarly to the study by Ling and Govindaraju. Both use the gamma distribution function, which has been comprehensively investigated in the author's former study about Using the Beta-Binomial Distribution for the Analysis of Biometric Identification [10, 11]. Both studies reveal the importance of two crucial mathematical details, such as the importance of the calculation method of the variables that determine the risk and the method of the fusion or summation of the modalities. Meanwhile the calculation of each modality's likelihood is a more conventional, yet not a simple task, as the fusion and the combined risk of the whole process is more complex.

Our former study found that the failed rejection rate depends on several variables, for which an explicit formula does not exist. As failures come from different subsets of mistakes and statistical uncertainty, the normal binomial fail estimation is not able to lead to the right consequences. For this reason a new 'p' variable has been chosen to the distribution of the probability, instead of a constant. With this methodology it is possible to characterize a biometric device on a smaller sample from a known population [11].

Many solutions have been investigated, but in this article a relatively new method is going to be shown. Human recognition cannot be described as a conventional binary logic, which was stated at first by L. A. Zadeh. Instead of a sharp 'yes' or 'no', the human mind distinguishes on an imaginary line, which Zadeh called the membership function [12].

As a part of soft-computing methods the Fuzzy Logic presents a set of ways of the fusion. Even more so, some variables in the fuzzy sets can be optimized with other soft computing methods, like neural networks or genetic algorithms. These techniques are bringing a new era into risk management with deep learning.

As it has been shown in robotics, the Fuzzy Implication is an appropriate technique for modeling human decisions. According to Takagi and Sugeno, the Fuzzy Implication spread worldwide in control applications and classifiers, and it is also a useful tool for predictions [13, 14].

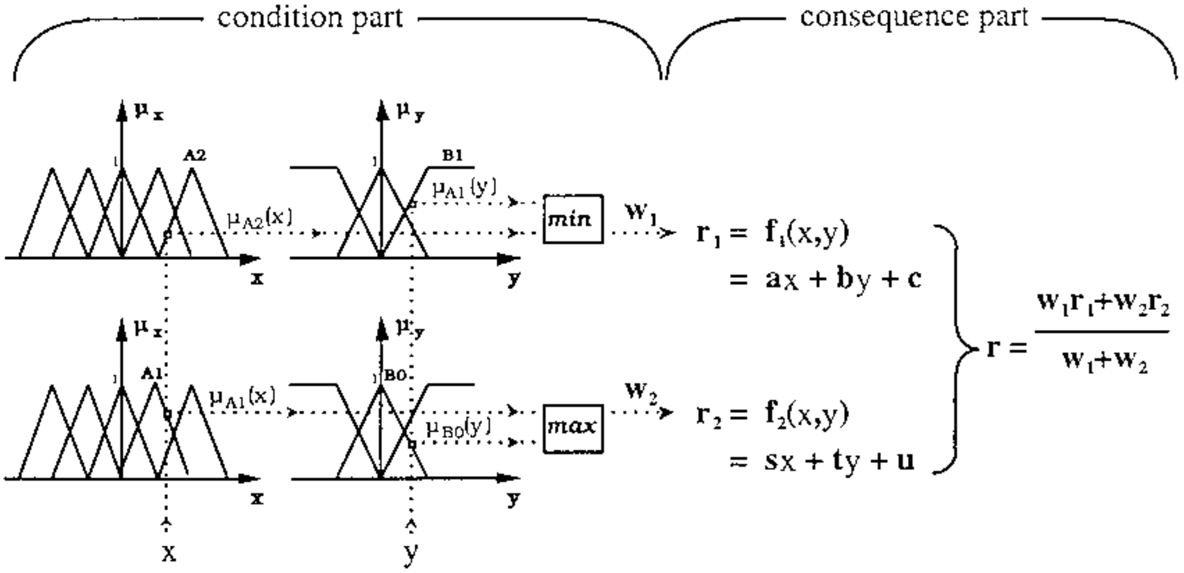

Figure 4. Takagi-Sugeno’s method [13].

Jyh-Shing Roger Jang has presented the way by which it is possible to blend Artificial Neural Networks (ANN) and Fuzzy Implications systems. Fuzzy Implications are practical to make decisions based on a preset fuzzy rule set, but in itself it is a static implication that has been created by experiences. If the fuzzy parameters could be changed and optimized to the exact situation, the fuzzy inference would be more precise. To make a system adaptable, it must be capable of being taught, which creates the need for learning. With ANN it is possible to preset the parameters of the algorithm during a teaching phase. As Wang presented the Error Back-propagation minimize the distance among the desired target and the current output. The most effective solution is a gradient descent method where the gradient is the vector of the partial derivatives from the parameter’s errors [15, 16].

As the authors have shown in Optimization of Big Population’s Multimodal Biometrical Identification with a Complex neuro-Fuzzy Logic Controller, the ANFIS (Adaptive Neuro-Fuzzy Inference System) can combine the different biometric modals by qualitative indexes and makes it possible to learn some changes in the environment. The implemented ANFIS was trained by a Resilient Back Propagation, which was more suitable as an error back propagation method for learning. The outcome has shown that it is possible to find the correct number of epochs where the difference of the desired and the current output is minimal [17].

In the implemented algorithm two different inputs have been set, representing two biometric modalities in the ANFIS. The analogy is the following: each incoming dataset has to be compared to the other modalities by benchmark index, which is correlated to the quality of the dataset. For instance, the quality of a fingerprint sample has to be compared to the iris modal’s quality. Following the comparison, the result of the ANFIS can determine the severity of the matching or the final decision which is made by the summing decision block.

RESULTS

With regard to the mathematical methods described above, a special combination of the statistical Bayes Theroem and a deterministic Soft Computing technique can describe an algorithm which is suitable and well-adapted to the typical failures of biometric identification. Figure 6 shows the mathematical framework of the implemented system.

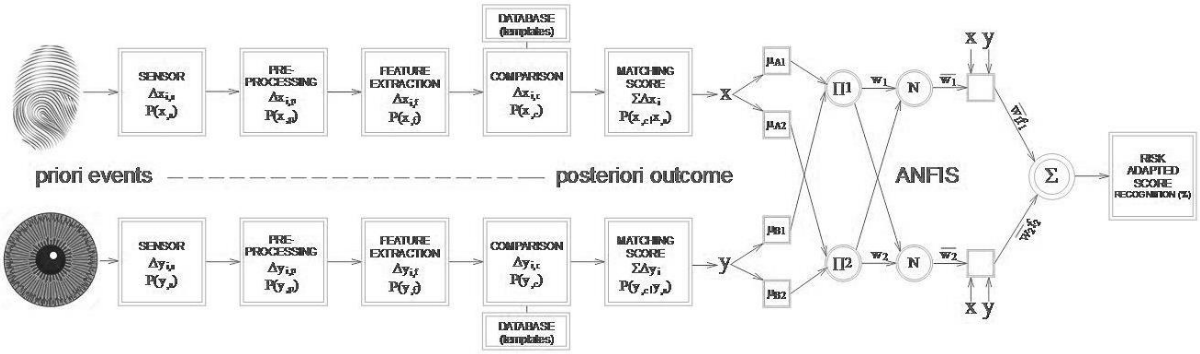

Figure 5. Algorithm of risk-adapted multimodal biometric identification.

The first part of the algorithm minimizes the effect of failure in the chain of the recognition process, while the second is a summation method that can be taught to detect the personal or local characteristics. The outcome is a risk adapted score, which is not a typical value, because it includes a correction unlike conventional biometrical outputs.

The method must be applied with caution, because there are preliminary steps that must be done properly, and tested before everyday use, just like in every solution that uses deep-learning.

CONCLUSIONS

The study has shown that the implementation of risk adaption in the authentication process is more than necessary, because the aggregated value of the risks can describe the suitable strength of the protocols. In some cases the boundaries of a biometric identification cannot be shifted with conventional methods, so it is worth using a multimodal process that can decrease the posteriori likelihood of systematic failures. The recognition can be even more accurate, if the scores of the matching passes through an ANFIS algorithm which has been taught in advance. Risk mitigation in the field of safety and security is a main objective, but usually there are only a few quantitative methods to decrease the invasive effect of natural impacts, such as environmental changes, human factor or frequent inadequate usage. With these modifications, the efficiency of access control systems can be increased, and the FRR and FAR can simultaneously improve. Therefore, the average time of access control can decrease even in highly secured installations.

REFERENCES

[1] Dolcourt, J.: *Vivo phone shows off first in-screen fingerprint scanner.* https://www.cnet.com/news/vivo-first-in-screen-fingerprint-scanner-for-phones-ces-2018, accessed 28th December 2018,

[2] NVIDIA Corporation: *Self-Driving Safety Report 2018.* https://www.nvidia.com/content/dam/en-zz/Solutions/self-driving-cars/safety-report/auto-print-safety-report-pdf-v16.5%20(1).pdf, accessed 28th December 2018

[3] Haimes, Y.Y.: *In: Risk Modeling, Assessment, and Management.* John Wiley & Sons, Hoboken, Ch.2, 2005, http://dx.doi.org/10.1002/9780470422489.ch2,

[4] Jain, A.K.; Nandakumar, K and Nagar, K.: *Biometric Template Security.* EURASIP Journal on Advances in Signal Processing **2008**, 1-17, 2008, http://dx.doi.org/10.1155/2008/579416,

[5] Roberts, C.: *Biometric attack vectors and defences.* Computer and Security, Department of Information Sciences **26**(1), 14-25, 2007, http://dx.doi.org/10.1016/j.cose.2006.12.008,

[6] Ratha, N.K.; Connell, J.H. and Bolle, R.M.: *An Analysis of Minutiae Matching Strength*. Proceedings of the 3rd International Conference on Audio and Video Based Biometric Person Authentication (AVBPA '01). Springer, Berlin, 2001, http://dx.doi.org/10.1007/3-540-45344-X_32,

[7] Srivastava, H.: *A Comparison Based Study on Biometrics for Human Recognition.* IOSR Journal of Computer Engineering **15**(1), 22-29, 2013, http://dx.doi.org/10.9790/0661-1512229,

[8] Maurer, D.E. and Baker, J.P.: *Fusing multimodal biometrics with quality estimates via a Bayesian belief network*. Journal Pattern Recognition **41**(3), 821-832, 2008, http://dx.doi.org/10.1016/j.patcog.2007.08.008,

[9] Maurer, D.E.; Baker, J. P.: *Fusion of biometric data with quality esitmates via a Bayesian belief network*. Proceedings of the Biometric Symposium, 2005,

[10] Rodrigues, R.N.; Ling, L.L. and Gondaraju, V.: *Roboustness of multimodal biometric fusion methods against spoof attacks*. Journal of Visual Languages and Computing **20**(3), 169-179, 2009, http://dx.doi.org/10.1016/j.jvlc.2009.01.010,

[11] Hanka, L. and Werner, G.: *Using the Beta-binomial Distribution for the Analysis of Biometric Identification*. 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY). IEEE, Subotica, 2015, http://dx.doi.org/10.1109/SISY.2015.7325381,

[12] Zadeh, L.A.: *Fuzzy Sets*. Information and Control **8**(3), 338-353, 1965, http://dx.doi.org/10.1016/S0019-9958(65)90241-X,

[13] Sugeno, M. and Takagi, T.: *Derivation of Fuzzy Control Rules from Human Operator's Control Actions*. IFAC Proceedings Volumes **16**(13), 55-60, 1983, http://dx.doi.org/10.1016/S1474-6670(17)62005-6,

[14] Sugeno, M. and Takagi, T.: *Fuzzy Identification of Systems and Its Application to Modeling and Control*. IEEE Transactions on Systems, Man, and Cybernetics **15**(1), 116-132, 1985, http://dx.doi.org/10.1109/TSMC.1985.6313399,

[15] Jang, J-S.R.: *Fuzzy Modeling Using Generalized Neural Networks and Kalman Filter Algorithm*. AAAI'91 Proceedings of the ninth National conference on Artificial intelligence **2**, pp.762-767, 1991,

[16] Wang, L.X. and Mendel, J.M.: *Back-propagation Fuzzy System as Nonlinear Dynamic System Identifiers.* IEEE International Conference on Fuzzy Systems. IEEE, San Diego, 1992, http://dx.doi.org/10.1109/FUZZY.1992.258711,

[17] Hanka, L. and Werner, G.: *Optimization of Big Population's Multimodal Biometrical Identification with a Complex neuro-Fuzzy Logic Controller*. Sixth International Scientific Videoconference of Scientists and PhD students or candidates **31**(5), 2017.